Estimation of the opacity degree of a system holding a secret

(Master thesis in Computer Science and Control)

Subject : We consider a dynamic system and some secret property defined over the runs of this system. For its interactions with the outside world, the system produces visible events and may also accept some inputs, which allows one to partially guess its internal behaviors. So autonomous or driven runs of the system may disclose some information about its secret property. The problem is to determine if the secret of the system is always preserved along its interactions (opacity problem), and to quantify the information leak about this secret (opacity degree evaluation).

More formally, the opacity problem is stated in the setting of discrete event systems, assuming models as automata, stochastic automata (or Markov chains), weighted automata, (weighted) Petri nets, etc. As a first step, one can assume the system does not accept inputs, but performs a hidden run in which only some transitions are visible (i.e. produce a visible event). The secret property can be expressed as a partition of the set of possible trajectories. The secret is revealed/discovered if, from the collected observations, an observer can determine which subset the hidden run belongs to. On the contrary, if ambiguity remains in all cases, the system is said to be opaque. In many situations of interest, the system can be weakly opaque, in the sense that given the collected observations, it is much more likely that the hidden run belongs to one subset than to another. Although the system is opaque in such situations, there is however a leak of information about the secret : an observer does not get all the necessary bits of information that would allow him to guess the hidden property with certainty, but he nevertheless gets part of these bits. An important issue is then to quantify this amount of revealed bits about the secret, and to measure as well how many bits away one is from knowing the secret. For systems accepting inputs, strategic considerations immediately appear as an attacker may want to drive the system in order to collect as much information as possible about the secret.

The objective of this internship is first of all to formalize adequately this (or these) question(s), and to design an algorithmic solution to estimate the opacity degree of a system. According to the accomplished progress, one may go as far as computing optimal strategies that extract the most information possible from an open system. The background will be a set of classical results about weighted/stochastic automata, for example algorithms to compute volumes of trajectory sets, and of course basic results in information theory.

Bibliography :

— B. Bérard, J. Mullins, M. Sassolas : "Quantifying Opacity," 7th International Conference on Quantitative Evaluation of Systems (QEST 2010), Williamsburg, Virginia, USA, pp. 263-272, 2010.

— Corinna Cortes, Mehryar Mohri, Ashish Rastogi, and Michael Riley : "On the computation of the relative entropy of probabilistic automata," International Journal of Foundations of Computer Science, 19(1) :219-242, 2008.

Contact : Eric Fabre, eric.fabre@inria.fr, +33 (0)2 99 84 73 26
http ://people.rennes.inria.fr/Eric.Fabre
http ://www.irisa.fr/sumo/index.html